

AMENDMENTS TO THE CLAIMS

Claim 1. (currently amended) An information recording/playback system for recording and playing back information, comprising:

an authentication data recording control part which provides control of detecting random pattern information based on random physical phenomena from a random-pattern-information recording part used for recording random pattern information based on random physical phenomena, creating medium identification information from the random pattern information, and recording, as authentication data, the medium identification information in an authentication data recording part on the information recording medium;

an authentication processing part which detects the random pattern information from the random-pattern-information recording part, creates medium-identification-information verification data from the random pattern information, reads authentication data from the authentication data recording part on the information recording medium, and performs authentication processing for the information recording medium based on medium-identification-information verification data created from the random pattern information and based on the authentication data; and

an information recording/playback control part which provides control of recording information on an information recording medium and playing back information from an information recording medium based on an authentication result from the authentication processing part;

wherein the authentication data recording control part records, as authentication data, the medium identification information together with a digital signature of a person

who recorded the medium identification information in the authentication data recording part on the information recording medium.

Claim 2. (original) The information recording/playback system according to claim 1, wherein there is further provided an encryption part which encrypts information by using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the information recording/playback control part provides control of recording information encrypted by the encryption part on the authenticated information recording medium.

Claim 3. (currently amended) The information recording/playback system according to claim 2, wherein the information recording/playback control part provides control of recording encrypted information and control of the encryption key used for information encryption on the authenticated information recording medium.

Claim 4. (original) The information recording/playback system according to claim 3, wherein the encryption part encrypts information using the encryption key and encrypts the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing,

wherein the information recording/playback control part provides control of recording information encrypted with the encryption key and the encrypted encryption key on the authenticated information recording medium.

Claim 5. (original) The information recording/playback system according to claim 2, wherein the encryption part creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 6. (original) The information recording/playback system according to claim 1, wherein there is further provided a decryption part for decrypting information by using medium identification information on an information recording medium authenticated by the authentication processing,

wherein the information recording/playback control part provides control of reading encrypted information from the authenticated information recording medium, and

wherein the decryption part decrypts encrypted information read by the information recording/playback control part from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 7. (currently amended) The information recording/playback system according to claim 6, characterized in that the information recording/playback control part provides control of reading encrypted information and control of the encryption key used for information encryption from the authenticated information recording medium.

Claim 8. (original) The information recording/playback system according to claim 7, wherein the information recording/playback control part provides control of reading encrypted information and the encrypted encryption key from the information recording medium, and wherein the decryption part decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

Claim 9. (canceled)

Claim 10. (currently amended) An information recording/playback system according to claim 9~~1~~, wherein the authentication data recording control part records a digital signature for a manufacturer of the information recording medium ~~as a digital signature for a recording person who recorded the medium identification information.~~

Claim 11. (currently amended) An information recording apparatus for recording information on an information recording medium including a random-pattern-information recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information generated according to random pattern information detected from the random-pattern-information recording part, wherein the information recording apparatus ~~is,~~ comprising comprises:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation part which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection part;

an authentication processing part which reads authentication data from an authentication data recording part on an information recording medium, performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data, and controls whether to write information onto an information recording medium based on an authentication result; and

a recording control part which provides control of recording information on an information recording medium; wherein the recording control part provides control of recording encrypted information and control of the encryption key used for information encryption on the authenticated information recording medium.

Claim 12. (original) The information recording apparatus according to claim 11, wherein there is further provided an encryption part which encrypts information by using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control part provides control of recording information encrypted by the encryption part on the authenticated information recording medium.

Claim 13. (canceled)

Claim 14. (currently amended) The information recording apparatus according to claim ~~13~~11, wherein the encryption part encrypts information by using the encryption key and encrypts the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control part provides control of recording information encrypted with the encryption key and control of the encrypted encryption key on the authenticated information recording medium.

Claim 15. (original) The information recording apparatus according to claim 12, characterized in that the encryption part creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 16. (currently amended) The information recording apparatus according to claim 11, wherein that the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a ~~recording~~ person who recorded the medium identification information based on the ~~recording~~ person's digital signature, and performs authentication processing with respect to an information

recording medium based on medium-identification-information verification data created by the verification data creation part and based on verified valid medium identification information.

Claim 17. (currently amended) The information recording apparatus according to claim 16, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 18. (currently amended) The information recording apparatus according to claim 16, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person together with the authentication data based on the revocation list.~~

Claim 19. (original) The information recording apparatus according to claim 18, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

Claim 20. (currently amended) An information playback apparatus for playing back information from an information recording medium including a random-pattern-information

recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part, wherein the information playback apparatus; comprises:

a random-pattern-information detection part which detects random pattern information from the random-pattern-information recording part on the information recording medium;

a verification data creation part which creates medium-identification-information verification data from random-pattern-information detected by the random-pattern-information detection part;

an authentication processing part which reads authentication data from the authentication data recording part and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data; and

a playback control part which provides control of reading information from an information recording medium;

wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a person who recorded the medium identification information based on the person's digital signature, and performs authentication processing with respect to

the information recording medium based on medium-identification-information
verification data created by the verification data creation part and based on verified valid
medium identification information.

Claim 21. (currently amended) The information playback apparatus according to claim 20, wherein the playback control part provides control of reading encrypted information from the authenticated information recording medium, and

wherein ~~the~~ a decryption part decrypts encrypted information read from the information recording medium by the playback control part by using medium identification information on the information recording medium authenticated by the authentication processing.

Claim 22. (currently amended) The information playback apparatus according to claim 21, wherein the playback control part provides control of reading encrypted information and control of an encryption key used for the information encryption from the authenticated information recording medium.

Claim 23. (original) The information playback apparatus according to claim 22, wherein the playback control part provides control of reading encrypted information and the encrypted encryption key from the authenticated information recording medium, and

wherein the decryption part decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

Claim 24. (canceled)

Claim 25. (currently amended) The information playback apparatus according to claim ~~24~~20, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 26. (currently amended) The information playback apparatus according to claim ~~24~~20, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person~~ together with the authentication data based on the revocation list.

Claim 27. (original) The information playback apparatus according to claim 26, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

Claim 28. (currently amended) An authentication data recording apparatus for recording authentication information on an information recording medium, comprising:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on an information recording medium for storing random pattern information based on random physical phenomena;

a medium identification information creation part which creates medium identification information from the random pattern information detected by the random-pattern-information detection part; and

an authentication data recording control part which provides control of recording, as authentication data, the medium identification information created by the medium identification information creation part in an authentication data recording part on the information recording medium; wherein the authentication data recording control part records, as authentication data, the medium identification information together with a digital signature for a person recording the medium identification information in an authentication data recording part on the information recording medium.

Claim 29. (canceled)

Claim 30. (original) The authentication data recording apparatus according to claim 28, characterized in that the authentication data recording control part records a digital signature for a manufacturer of the information recording medium ~~as a digital signature for a recording person of the medium identification information.~~

Claim 31. (original) The authentication data recording apparatus according to claim 28, wherein the authentication data recording control part records a revocation list about a manufacturer together with the authentication data in an authentication data recording part on the information recording medium.

Claim 32. (currently amended) An authentication processing apparatus for performing authentication processing with respect to an information recording medium, comprising:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on the information recording medium;

a verification data creation part which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection part; and

an authentication processing part which reads authentication data from an authentication data recording part on the information recording medium and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data; wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a person who recorded the medium identification information based on the person's digital signature, and performs

authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation part and based on verified valid medium identification information.

Claim 33. (canceled)

Claim 34. (currently amended) The authentication processing apparatus according to claim 33~~32~~, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 35. (currently amended) The authentication processing apparatus according to claim 33~~32~~, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person~~ together with the authentication data based on the revocation list.

Claim 36. (original) The authentication processing apparatus according to claim 35, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

Claim 37. (currently amended) The authentication processing apparatus according to claim 35, wherein the authentication processing part has a storage part, stores a ~~recording~~ person's identification information and a public key thereof for a manipulated information recording medium together with a revocation flag, updates the revocation flag using a new revocation list, and performs authentication processing based on the revocation list stored in the storage part.

Claim 38. (currently amended) An information recording/playback method for recording and playing back information, comprising:

an authentication data recording control process which provides control of detecting random pattern information based on random physical phenomena from a random-pattern-information recording part for recording random pattern information based on random physical phenomena on an information recording medium, creating medium identification information from the random pattern information, and recording, as authentication data, the medium identification information in an authentication data recording part on the information recording medium;

an authentication process which detects the random pattern information from the random-pattern-information recording part, creates medium-identification-information verification data from the random pattern information, reads authentication data from the authentication data recording part on the information recording medium, and performs authentication processing with respect to the information recording medium based on

medium-identification-information verification data created from the random pattern information and based on the authentication data; and

an information recording/playback control process which provides control of recording information on an information recording medium and playing back information from an information recording medium based on an authentication result from the authentication processing process;

wherein the authentication data recording control process records, as authentication data, the medium identification information together with a digital signature for a person recording the medium identification information in an authentication data recording part on the information recording medium.

Claim 39. (original) The information recording/playback method according to claim 38, wherein there is further provided an encryption process which encrypts information using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the information recording/playback control process provides control of recording information encrypted by the encryption process on the authenticated information recording medium.

Claim 40. (currently amended) The information recording/playback method according to claim 39, wherein the information recording/playback control process provides control of recording encrypted information and control of the encryption key used for information encryption on the authenticated information recording medium.

Claim 41. (currently amended) The information recording/playback method according to claim 40, wherein the encryption process encrypts information using the encryption key and encrypts the encryption key used for information encryption using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the information recording/playback control process provides control of recording information encrypted with the encryption key and control of the encrypted encryption key on the authenticated information recording medium.

Claim 42. (original) The information recording/playback method according to claim 39, wherein the encryption process creates the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 43. (original) The information recording/playback method according to claim 38, wherein the information recording/playback control process provides control of reading encrypted information from the authenticated information recording medium, and

wherein the decryption process decrypts encrypted information read by the information recording/playback control process from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 44. (currently amended) The information recording/playback method according to claim 43, wherein the information recording/playback control process provides control of reading encrypted information and control of the encryption key used for information encryption from the authenticated information recording medium.

Claim 45. (currently amended) The information recording/playback method according to claim 44, wherein the information recording/playback control process provides control of reading encrypted information and control of the encrypted encryption key from the authenticated information recording medium, and

wherein the decryption process decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

Claim 46. (canceled)

Claim 47. (currently amended) The information recording/playback method according to claim 4638, wherein the authentication data recording control process records a digital signature for a manufacturer of the information recording medium as a digital signature for a ~~recording~~ the person of ~~recording~~ the medium identification information.

Claim 48. (currently amended) An information recording method for recording information on an information recording medium including: a random-pattern-information

recording part which records random pattern information based on random physical phenomena;
and an authentication data recording part which stores, as authentication data, medium
identification information created according to random pattern information detected from the
random-pattern-information recording part, wherein the information recording method,
comprising:

a random-pattern-information detection process which detects random pattern
information from a random-pattern-information recording part on an information
recording medium;

a verification data creation process which creates medium-identification-
information verification data from random pattern information detected by the random-
pattern-information detection process;

an authentication process which reads authentication data from the authentication
data recording part on an information recording medium, performs authentication
processing for an information recording medium based on medium-identification-
information verification data created by the verification data creation process and based
on the authentication data, and controls whether to enable writing information onto an
information recording medium based on an authentication result; and

a recording control process which provides control of recording information onto
an information recording medium;

wherein the authentication process verifies validity of the medium identification
information with respect to an information recording medium which records, as
authentication data, the medium identification information together with a digital
signature of a person who recorded the medium identification information based on the

person's digital signature, and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

Claim 49. (original) The information recording method according to claim 48, wherein there is further provided an encryption process which encrypts information using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the recording control process provides control of recording information authenticated by the encryption process on the authenticated information recording medium.

Claim 50. (original) The information recording method according to claim 49, characterized in that the recording control process provides control of recording encrypted information and the encryption key used for information encryption on an authenticated information recording medium.

Claim 51. (currently amended) The information recording method according to claim 50, wherein the encryption process encrypts information using the encryption key and encrypts the encryption key used for information encryption using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control process provides control of recording information encrypted with the encryption key and control of the encrypted encryption key on the authenticated information recording medium.

Claim 52. (original) The information recording method according to claim 49, wherein the encryption process creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 53. (canceled)

Claim 54. (currently amended) The information recording method according to claim ~~53~~48, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 55. (currently amended) The information recording method according to claim ~~53~~48, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person~~ together with the authentication data based on the revocation list.

Claim 56. (original) The information recording method according to claim 55, wherein the authentication process stores a revocation list recorded on an information recording medium when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

Claim 57. (currently amended) An information playback method for playing back information from an information recording medium including a random-pattern-information recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part, wherein the information playback method, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation process which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection process;

an authentication process which reads authentication data from the authentication data recording part on an information recording medium and performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on the authentication data; and

a playback control process which provides control of reading information from an information recording medium;

wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a person who recorded the medium identification information based on the person's digital signature, and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

Claim 58. (currently amended) The information playback method according to claim 57, wherein the playback control process provides control of reading encrypted information from the authenticated information recording medium, and

wherein ~~the~~ a decryption process decrypts encrypted information read by the playback control process from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

Claim 59. (currently amended) The information playback method according to claim 58, wherein the playback control process provides control of reading encrypted information and control of the encryption key used for information encryption from the authenticated information recording medium.

Claim 60. (currently amended) The information playback method according to claim 59, wherein the playback control process provides control of reading encrypted information and control of the encrypted encryption key from the information recording medium, and

wherein the decryption process decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

Claim 61. (canceled)

Claim 62. (currently amended) The information playback method according to claim ~~61~~57, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 63. (currently amended) The information playback method according to claim ~~61~~57, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person~~ together with the authentication data based on the revocation list.

Claim 64. (original) The information playback method according to claim 63, wherein the authentication process stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

Claim 65. (currently amended) An authentication data recording method for recording authentication information on an information recording medium, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium storing random pattern information based on random physical phenomena;

a medium identification information creation process which creates medium identification information from the random pattern information detected by the random-pattern-information detection process; and

an authentication data recording control process which provides control of recording, as authentication data, the medium identification information created by the medium identification information creation process in an authentication data recording part on the information recording medium; wherein the authentication data recording control process records, as authentication data, the medium identification information together with a digital signature for a person recording the medium identification information in an authentication data recording part on the information recording medium.

Claim 66. (canceled)

Claim 67. (currently amended) The authentication data recording method according to claim ~~66~~65, wherein the authentication data recording control process records a digital signature for a manufacturer of the information recording medium ~~as a digital signature for a recording person of the medium identification information.~~

Claim 68. (original) The authentication data recording method according to claim 65, wherein the authentication data recording control process records a revocation list about a manufacturer together with the authentication data in an authentication data recording part on the information recording medium.

Claim 69. (currently amended) An authentication processing method for performing authentication processing with respect to an information recording medium, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation process which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection process; and

an authentication process which reads authentication data from the authentication data recording part on an information recording medium and performs authentication processing for an information recording medium based on medium-identification-

information verification data created by the verification data creation process and based on the authentication data; wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a person who recorded the medium identification information based on the person's digital signature, and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

Claim 70. (canceled)

Claim 71. (currently amended) The authentication processing method according to claim ~~70~~69, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium ~~as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.~~

Claim 72. (currently amended) The authentication processing method according to claim ~~70~~69, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list ~~about a recording person~~ together with the authentication data based on the revocation list.

Claim 73. (original) The authentication processing method according to claim 72, wherein the authentication process stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

Claim 74. (currently amended) The authentication processing method according to claim 72, wherein the authentication process stores a ~~recording~~ person's identification information and a public key thereof for a manipulated information recording medium together with a revocation flag, updates the revocation flag using a new revocation list, and performs authentication processing based on the revocation list stored in the storage process.

Claim 75. (currently amended) An information recording medium for recording information, comprising:

a random-pattern-information recording part which records random pattern information based on random physical phenomena;

an authentication data recording part which stores, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part; and

an information recording part which records information;

wherein the authentication data recording part records the medium identification information as authentication data together with a digital signature for a person recording the medium identification information.

Claim 76. (canceled)

Claim 77. (currently amended) The information recording medium according to claim ~~76~~75, wherein the authentication data recording part records a digital signature for a manufacturer of the information recording medium ~~as a digital signature for a recording person of the medium identification information.~~

Claim 78. (original) The information recording medium according to claim 77, wherein the authentication data recording part records a revocation list about a manufacturer together with the authentication data.